Universidade Federal de Campina Grande
Departamento de Engenharia Elétrica
Coordenação de Graduação em Engenharia Elétrica

Trabalho de Conclusão de Curso

Estudo e Análise de um Sistema de IP Móvel em Linux

Danilo Freire de Souza Santos
danilo.santos@grad.dee.ufcg.edu.br

Orientador:
Angelo Perkusich

Campina Grande, Junho de 2005

Biblioteca Setorial do CDSA. Fevereiro de 2021.

Sumé - PB

Glossário

ARP - Address Resolution Protocol
CN - Correspondent Node
DNS - Domain Name System
DHCP - Dynamic Host Configuration Protocol
GSM - Global System Mobile
HLR - Home Location Register
HTTP - Hypertext Transfer Protocol
IETF - Internet Engineering Task Force
IP - Internet Protocol
IPv4 - Internet Protocol versão 4
IPv6 - Internet Protocol versão 6
MAC - Media Access Control
MD5 - Message Digest 5
MIP - Mobile IP
MLR - Mobile Location Register
NTP - Network Time Protocol
OS - Operational System
QoS - Quality of Service
RFC - Request For Comments
RTP - Real Time Protocol
TCP - Transport Control Protocol
TMIP - Transparent Mobile IP
TTL - Time To Live
UDP - User Datagram Protocol
VoIP - Voz over IP
Wi-Fi - Wireless Fidelity
xDSL - Digital Subscriber Line

Resumo

Este trabalho apresenta uma introdução sobre o conceito de IP Móvel, mostrando as recomendações propostas pelo IETF para o suporte a mobilidade na Internet. O principal objetivo deste trabalho, porém, é estudar e analisar um sistema de IP Móvel. Para isso, é exposto um cenário para implantação e parâmetros de comparação e desempenho para uma análise comparativa. Em seguida é exposto os aspectos e detalhes do sistema de IP Móvel escolhido, o TMIP. Nesta exposição são detalhados os parâmetros de configuração e funcionamento do sistema, apontando suas vantagens e seus problemas.

Conteúdo

Lista de Figuras

Capítulo 1

Introdução

Com a universalização das comunicações e a cada vez maior necessidade de acesso à informação em qualquer lugar e a qualquer hora, existe cada vez mais a necessidade de incorporar mobilidade às aplicações. Esta necessidade de acesso a informação em qualquer lugar e hora vem dos avanços da tecnologia de rádio freqüência, da explosão de vendas de *laptops* e PDAs e também dos novos modelos de negócio que necessitam e confiam na disponibilidade de informação instantânea.

Vale ressaltar que mobilidade não deve ser confundida com portabilidade. Portabilidade pode ser exemplificada como softwares que são executados em um dispositivo móvel, mas que não necessitam estarem conectados a uma rede. Em uma rede com suporte à mobilidade, atividades computacionais não devem ser interrompidas quando o usuário troca o ponto de conexão.

A solução em hardware para tais necessidades já existe: computadores pessoais e *notebooks* podem ser equipados com *modens* dos mais diversos tipos (xDSL, GSM, etc.), ou com placas de rede sem fio (Wi-Fi, Bluetooth, etc.). Contudo, os protocolos e softwares requeridos para comunicação móvel que são usados com esses hardwares, não são totalmente difundidos e disponíveis. Os protocolos usualmente usados, incluindo os da pilha TCP/IP (IPv4), foram feitos

assumindo que computadores estão sempre conectados a rede por um ponto físico fixo [2]. Quando um computador móvel não está fisicamente conectado com sua sub-rede de origem, o protocolo IPv4 é incapaz de rotear os pacotes corretamente. Para resolver esse problema seria necessário que um desses procedimentos fosse executado:

- O nó teria de mudar seu endereço IP toda vez que mudasse seu ponto de conexão à rede;
- Um novo caminho de conexão deveria ser procurado por toda a Internet, para se achar o nó com endereço de IP especificado.

Porém nenhuma dessas soluções é praticável. Em relação à primeira, como foi dito anteriormente o protocolo IPv4 rotea pacotes para seus destinos de acordo com o endereço IP. Estes endereços são associados com um endereço fixo de rede. Quando o destino de um pacote é um nó móvel, isto significa que cada novo ponto de conexão feito pelo nó móvel é associado com uma nova rede e, portanto, com um novo endereço IP. Isto torna a mobilidade impossível, pois para manter as conexões existentes na camada de transporte ativas enquanto um nó móvel muda de um lugar para outro, é necessário manter o mesmo endereço IP. No TCP, que é responsável pela maioria das conexões na Internet, conexões são indexadas por quatro números, que são os endereços IP e os números das portas dos nós de origem e destino. Mudando qualquer um desses números a conexão será interrompida e perdida.

Em relação à segunda solução, observam-se problemas óbvios de escalabilidade quando se trata de uma rede como a Internet. Pois:

- É impossível propagar uma rota especifica para um nó por toda a Internet;
- A atualização da rota pode ser muito freqüente enquanto o nó se move;
- O número dessas rotas específicas é muito grande com o aumento do número de dispositivos móveis.

Então, para resolver esses problemas foi especificado um novo protocolo, o MIP (*Mobile IP*), que modifica o protocolo IPv4 para que a mobilidade possa ocorrer transparentemente para as camadas mais altas. O IP Móvel, que é especificado na recomendação RFC 2002 [8], é um padrão proposto por um grupo de trabalho do IETF (*Internet Engineering Task Force*). Seus propósitos envolveram vários *Internet Drafts*, o que levou a alguns novos protocolos: Suporte a Mobilidade IP [8], Otimização de roteamento no IP Móvel, Encapsulamento IP em IP [7] e Mínimo Encapsulamento IP [9]. Suporte a Mobilidade IP é o protocolo base - chamado de IP Móvel. Ele propõe uma solução para resolver o problema de mobilidade em redes IP permitindo que o nó móvel use dois endereços IP: um endereço fixo de origem e um endereço de tratamento que muda a cada novo ponto de conexão.

Neste trabalho é exposto o funcionamento do IP Móvel. São analisadas as implementações existentes para o sistema operacional Linux em relação a um cenário de implantação proposto. Ao final o sistema escolhido de IP Móvel será exposto e discutido.

O restante deste documento está organizado da seguinte forma: No Capítulo 2, são explicados os princípios do IP Móvel em sua versão IPv4, incluindo a nova arquitetura proposta pela RFC 2002 e o seu funcionamento. Em seguida será feita uma comparação entre o IPv4 Móvel e o suporte à mobilidade da nova versão do protocolo IP, o IPv6, explicitando as principais diferenças e vantagens do novo protocolo. No Capítulo 3, são analisados os sistemas de IP Móvel para o sistema operacional Linux pesquisados. A partir desta análise será escolhido um sistema para estudo o qual se adapte à topologia de rede proposta, que é exposta na análise de cenário de implantação. No Capítulo 4, é analisado e exposto o sistema de IP Móvel Transparente (*Transparent Mobile IP* [1]), enfatizando seus parâmetros de configuração, arquitetura e funcionamento. Por final, no Capítulo 5 é examinado o andamento do trabalho atual e apresentado as conclusões referentes ao sistema de IP Móvel especificado pelo IETF.

Capítulo 2

O IP Móvel

Como dito no capítulo anterior, o IPv4 assume que um endereço IP é unicamente identificado pelo seu ponto físico de conexão com a Internet. Pacotes destinados para um nó móvel não são entregues corretamente se ele estiver conectado a uma sub-rede externa. Portanto, para manter a conectividade com a Internet, outras entidades de rede são introduzidas junto ao nó móvel.

No entanto antes de explicar o funcionamento do IP Móvel, é interessante conhecer a terminologia usada neste trabalho [10] [11]. Estes termos serão usados extensivamente no decorrer do texto na descrição da operação do IP Móvel e dos processos de troca de mensagens entre as novas entidades de rede e entre os nós móveis.

Nó Móvel: Um nó executando a pilha de protocolo do IP Móvel que se movimenta entre diferentes sub-redes. Este nó tem um endereço IP, permanente, que define para onde todos os seus pacotes devem ser enviados. Quando outros nós enviam pacotes ao nó móvel, eles apenas especificam seu endereço IP de origem no pacote, não importando onde o nó móvel esteja fisicamente localizado.

Rede Externa: uma rede, diferente da rede de origem do nó móvel, a qual o mesmo está conectado.

Agente de Origem: um roteador na rede de origem que é responsável por interceptar e encaminhar os pacotes destinados para o nó móvel quando este está conectado a uma rede externa.

Endereço de Tratamento: o endereço que o no móvel usa para comunicação quando está fora de sua rede de origem. Este endereço pode ser tanto um endereço de tratamento de agente externo, quanto um endereço de tratamento arranjado (*collocated*), onde na interface de rede do nó móvel é temporariamente atribuído um endereço IP da rede externa.

Agente Externo: um roteador na rede externa configurado para IP Móvel. Ele auxilia o nó móvel recebendo *datagramas* enviados ao endereço de tratamento.

Nó Correspondente: qualquer ponto que está se comunicando com o nó móvel. Este nó pode estar localizado na rede local, na rede externa, ou qualquer outro lugar que seja capaz de rotear pacotes para a rede de origem do nó móvel.

Tunelamento: o processo de encapsular um pacote IP dentro de outro pacote IP com o propósito de roteá-lo para uma localização diferente da especificada no campo de destino original. Mais especificamente, quando um pacote é recebido pelo agente de origem, ele encapsula o pacote original dentro de outro pacote, colocando o endereço de tratamento como novo destino antes de encaminhá-lo para o roteador apropriado. O caminho seguido pelo novo pacote é chamado de *túnel*.

2.1 Funcionamento do IP Móvel

No IP Móvel, o endereço IP de origem também é estático e é usado, por exemplo, para identificar conexões TCP. O endereço de tratamento muda a cada novo

ponto de conexão e pode ser visto como endereço topológico real do nó móvel. Ele indica o número de rede e, portanto o ponto de conexão do nó móvel em relação à topologia da rede. O endereço de origem faz parecer que o nó móvel está continuamente capaz de receber dados em sua rede de origem, onde o IP Móvel requer a existência de um agente de origem. Quando o nó móvel não estiver conectado à sua rede de origem, o agente de origem captura todos os pacotes destinados para o nó móvel e os envia para o ponto de conexão atual do mesmo.

Quando o nó móvel se movimenta, ele registra seu novo endereço de tratamento com seu agente de origem. Desta forma, o agente de origem entrega os pacotes destinados ao endereço de origem para o endereço de tratamento. Para fazer a entrega, necessita-se que o pacote seja modificado para que o endereço de tratamento apareça como endereço IP de destino. Esta modificação pode ser entendida como uma transformação de pacote ou, mais especificamente, um redirecionamento. Quando o pacote chega ao endereço de tratamento, a transformação reversa é aplicada para que o pacote novamente tenha o endereço de origem do nó móvel como endereço IP de destino. Quando o pacote chega ao nó móvel associado ao endereço de origem, ele será corretamente processado pelo TCP ou qualquer outro protocolo de nível superior. Portanto o IP Móvel é melhor entendido como a cooperação de três mecanismos [10]:

- Descobrimento do endereço de tratamento;
- Registro do endereço de tratamento;
- Encapsulamento e tunelamento de pacotes.

2.2 Descobrimento do Endereço de Tratamento

O processo de descoberta do IP Móvel foi construído utilizando um protocolo padrão já existente, o protocolo de Anúncio de Roteador (*Router Advertise-*

ment), especificado na RFC 1256 [3]. O processo de descoberta no IP Móvel não modifica os campos originais do protocolo existente, mas simplesmente o estende, agregando as funções de mobilidade. Portanto, um anúncio de roteador pode carregar informações sobre roteadores padrões, como antes, e em adição carregar algumas informações sobre um ou mais endereços de tratamento. Essa extensão do anúncio de roteador contendo informações do endereço de tratamento é chamada de anúncio de agente. Agentes de origem e agentes externos tipicamente *broadcast* anúncios de agente em intervalos regulares. Se um nó móvel necessita de um endereço de tratamento e não deseja esperar pelo aviso periódico, o nó móvel pode fazer uma solicitação em *broadcast* ou *multicast* que será respondida por qualquer agente de origem ou agente externo que a receba. Portanto, um anúncio de agente realiza as seguintes funções:

- Permite a detecção de agentes de mobilidade;
- Lista um ou mais endereços de tratamento disponíveis;
- Informa ao nó móvel sobre características especiais providas pelo agente externo, como por exemplo, técnicas alternativas de encapsulamento;
- Faz os nós móveis determinarem o número de rede e o estado de seus links com a Internet;
- Informa ao nó móvel se ele está em sua rede de origem ou numa rede externa.

Como dito, o nó móvel usa esses avisos para determinar se ele moveu-se para uma nova localização e se ele pode conectar-se a essa rede. Caso ele ainda esteja conectado a sua rede local, nenhuma alteração é feita e nenhuma mudança na operação do protocolo IP é requerida para comunicação. Se o nó determina que está em uma rede externa, ele obtém um endereço de tratamento do agente externo, ou por outro protocolo tal como o DHCP (*Dynamic Host Configuration Protocol*, utiliza um endereço de tratamento arranjado. Quando usando um endereço de tratamento do agente externo, este é responsável por desempacotar os

pacotes tunelados mandados para ele pelo agente de origem do nó móvel, e após desempacotá-los envia os pacotes para o nó móvel. Ele também é responsável pelo redirecionamento de pacotes do nó móvel para o restante da rede. Alternativamente, o nó móvel pode estar diretamente conectado com a rede externa e portanto comunicando-se diretamente com o agente de origem. O uso de endereço de tratamento do agente externo é preferencial no IPv4 por causa do seu espaço de endereço limitado.

Os nós móveis utilizam as solicitações dos roteadores, como definido na RFC 1256, para detectar qualquer mudança no conjunto dos agentes de mobilidade disponíveis no ponto de conexão atual. Se os anúncios não são mais detectáveis vindos do agente externo, o nó móvel presume que o agente externo não está mais dentro da área da sua interface de rede. Nesta situação, o nó móvel começa a busca por um novo endereço de tratamento, ou possivelmente usa um endereço de tratamento conhecido, obtido de anúncios que ele ainda está recebendo. O nó móvel pode escolher por esperar por outro anúncio caso ele não tenha recebido qualquer anúncio de endereço de tratamento recentemente, ou pode continuar enviando uma solicitação de agente.

2.3 Registrando o Endereço de Tratamento

Uma vez que o nó móvel tenha um endereço de tratamento, seu agente de origem deve tomar conhecimento. A Figura 2.1 ilustra o processo de registro definido pelo IP Móvel. O processo começa quando o nó móvel, possivelmente com a assistência de um agente externo, envia uma requisição de registro com a informação de endereço de tratamento. Quando o agente de origem recebe esta requisição, ele adiciona a informação necessária à sua tabela de roteamento, aprova a requisição, e envia uma resposta ao nó móvel. Apesar do agente de origem não ser requisitado pelo protocolo de IP Móvel para lidar com requisições de registro, isso se faz uma estratégia natural de implementação, e a maioria das implementações utilizam

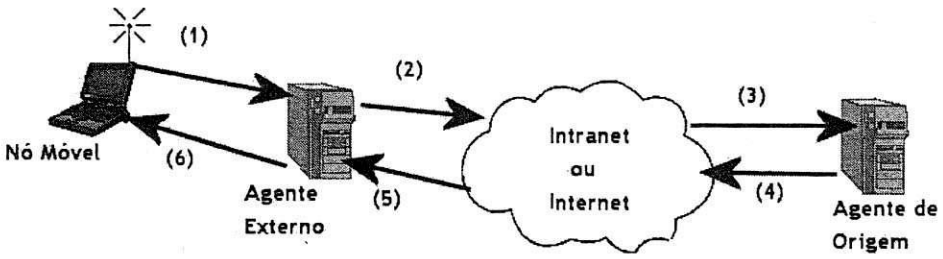

Figura 2.1: Processo de Registro do IP Móvel

essa abordagem. O processo é descrito da seguinte maneira:

1. O nó móvel envia uma requisição de registro de endereço de tratamento ao agente de origem;
2. O agente externo repassa essa informação para o agente de origem;
3. O agente de origem recebe a requisição;
4. O agente de origem envia uma resposta ao nó móvel;
5. O agente externo intercepta essa resposta;
6. O agente externo redireciona o pacote para o nó móvel.

Em relação à autenticação, as requisições de registro contêm parâmetros que caracterizam o túnel pelo qual o agente de origem irá entregar pacotes para o endereço de tratamento. Túneis podem ser construídos de várias maneiras, descritas na próxima seção. Quando um agente de origem aceita a requisição, ele começa associando o endereço de origem do nó móvel com o endereço de tratamento, e mantém essa associação até que o período de registro expire. A tripla que contém o endereço de origem, o endereço de tratamento, e o período de registro é chamada de ligação (*binding*) para o nó móvel. Uma requisição de registro pode ser considerada uma atualização de ligação enviada pelo nó móvel.

Uma atualização de ligação é um exemplo de redirecionamento remoto, pois ela é enviada remotamente para o agente de origem para atualizar a tabela de roteamento do mesmo. Esta abordagem de registro cria a necessidade de autenticação. O agente de origem deve ter certeza que o registro foi originado pelo nó móvel e não por outro nó qualquer. Um nó mal intencionado pode fazer o agente de origem alterar sua tabela de roteamento com informações de endereço de tratamento incorretas, e o nó móvel pode ficar inalcançável para toda comunicação vinda da Internet.

A necessidade de autenticar as informações de registro foi um grande problema na determinação de um projeto de parâmetros aceitável para o IP Móvel. Cada nó móvel e agente de origem deve compartilhar uma chave segura. Também devem ser capazes de usar o *Message Digest 5* (RFC 1321) [12] com uma chave de 128-*bits* para criar assinaturas digitais para requisições de registro. A assinatura é determinada pela execução do algoritmo MD5 sobre todos os dados dentro do cabeçalho da mensagem de registro e as extensões que precedem a assinatura [10].

Para a segurança da requisição de registro, cada requisição deve conter dados únicos para que dois registros diferentes nunca tenham em termos práticos o mesmo *hash* MD5. Por outro lado, o protocolo fica susceptível a ataques de repetição, no qual um nó malicioso pode gravar registros válidos para uma repetição posterior, acabando com a capacidade do agente de origem de tunelar para o atual endereço de tratamento do nó móvel posteriormente. Para assegurar que isto não ocorra, o IP Móvel acrescenta dentro da mensagem de registro um campo de identificação especial que muda a cada novo registro. A semântica exata do campo de identificação depende de vários detalhes, que são descritos na especificação do protocolo. Rapidamente, existem duas maneiras de fazer o campo de identificação único. Uma maneira é usando selos de tempo, onde cada novo registro terá um selo de tempo posterior e com isso se diferenciando de registros anteriores. A outra maneira é fazendo a identificação através de um

número pseudo-aleatório, então, com bits suficientes de aleatoriedade, é bastante improvável que dois valores independentes escolhidos para o campo de identificação sejam os mesmos. Quando a aleatoriedade é usada, o IP Móvel define um método que protege tanto a requisição de registro quanto a resposta de ataques de repetição. Se o nó móvel e o agente de origem estão bastante fora de sincronismo para o uso de selos de tempo, ou se eles perdem a contagem dos números aleatórios esperados, o agente de origem irá rejeitar o registro e incluir informação para re-sincronismo dentro da resposta. Usando números aleatórios ao invés de selos de tempo evita-se problemas de ataques ao protocolo NTP (*Network Time Protocol*), que podem levar o nó móvel a perder sincronismo com o agente de origem. Evita-se ainda que requisições de registro autenticadas possam ser usadas por um nó mal intensionado para subverter registros futuros.

O campo de identificação é também usado pelo agente externo para identificar requisições de registro pendentes com respostas de registro quando elas chegam do agente de origem, para assim ser capaz de re-enviar a resposta ao nó móvel. O agente externo também guarda outras informações para registros pendentes, incluindo o endereço de origem do nó móvel, endereço MAC do nó móvel, o número da porta para requisições de registro do nó móvel, o período de registro sugerido pelo nó móvel, e o endereço do agente de origem. O agente externo pode limitar o período de registro para um valor configurável, o qual ele coloca dentro dos anúncios de agentes. O agente de origem pode reduzir o período de registro que ele coloca como parte da resposta de registro, mas nunca pode aumentá-lo.

Como ilustrado na Figura 2.1, no IP Móvel os agentes externos são os mais passivos, repassando requisições e respostas de registros entre o agente de origem e o nó móvel. O agente externo também desencapsula tráfego de um agente de origem e o envia ao nó móvel. Note que os agentes externos não têm que ser autenticados para o nó móvel ou agente de origem. Então um agente externo qualquer pode lançar anúncios de agentes ao nó móvel, e pode se recusar a enviar pacotes desencapsulados ao nó móvel. Entretanto, este resultado não é pior do

que quando um nó é enganado a usar um roteador errado, o que é possível usando anúncios de roteadores não autenticados, como é especificado na RFC 1256.

Quando um nó móvel não consegue contatar o seu agente de origem, o mesmo tenta registrar-se com outro agente em sua rede de origem. Este método de descoberta automática de agente de origem funciona usando-se como alvo de registro um endereço IP de *broadcast* ao invés do endereço IP do agente de origem. Quando o pacote de *broadcast* chega à rede de origem, outro agente de origem irá mandar uma rejeição ao nó móvel, porém, nesta rejeição irá conter seu endereço para que assim o nó móvel possa usá-lo numa próxima tentativa de registro.

2.4 Encapsulamento e Tunelamento de Pacotes

Para o agente de origem enviar pacotes para o nó móvel quando ele estiver localizado fora de sua rede de origem, ele faz uso do encapsulamento. Quando um nó correspondente quer enviar um pacote ao nó móvel, ele utiliza apenas o endereço de origem permanente do nó móvel para enviar o pacote à rede de origem. O agente de origem intercepta este pacote e o encapsula em um novo pacote. Este novo pacote tem o endereço de tratamento do nó móvel como destino para que assim possa ser enviado para rede externa. O agente externo recebe esse pacote, já que ele é identificado como destino, e desencapsula o pacote original para encaminhá-lo ao nó móvel. Por fim, se o nó móvel quiser se comunicar com o nó correspondente, ele pode enviar os pacotes diretamente ao nó através do agente externo usando seu endereço IP de origem como endereço fonte do pacote. Esta rotina de tarefas é chamada de roteamento triangular. O processo de encapsulamento e tunelamento é descrito na Figura 2.2:

1. Pacote destinado ao nó móvel (NM) chega ao agente de origem;

2. O agente de origem faz um encapsulamento e tunela o pacote ao agente de origem. O número 4 indica que os dados do pacote são outro pacote IP e o

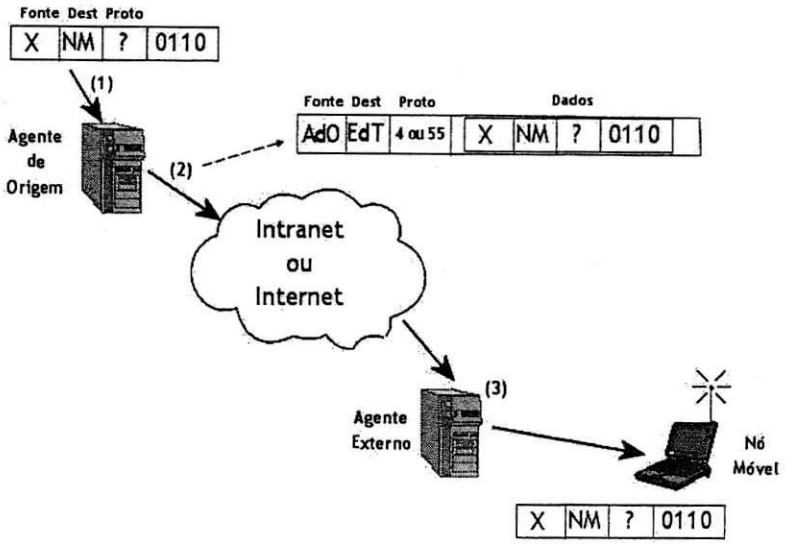

Figura 2.2: Processo de Encapsulamento e Tunelamento

número 55 indica mínimo encapsulamento IP;

3. O agente externo recebe o novo pacote, o desencapsula, e o envia ao nó móvel.

Alguns dos pacotes vindos de um nó correspondente podem ser roteados por caminhos mais longos para que possam ser roteados à rede de origem. Este é um pequeno preço a ser pago para se ter à vantagem do nó correspondente não necessitar de qualquer tipo de extensão para IP Móvel. Num tópico posterior serão mostradas extensões de roteamento do IP Móvel que aperfeiçoam o trajeto e requerem pequenas mudanças no nó correspondente.

Existem três tipos de encapsulamento que o agente de origem pode usar para o IP Móvel: encapsulamento IP-em-IP, encapsulamento mínimo, e encapsulamento de roteamento genérico. O encapsulamento IP-em-IP cria um novo pacote com a seção de informação (dados) do pacote contendo o pacote original. Isto acrescenta 20 *bytes* de sobrecarga para o tunelamento, mas tem a vantagem de que o pacote resultante é exatamente igual a qualquer outro pacote IP e pode

passar por processos intermediários de rede tais como fragmentação. O encapsulamento mínimo parte do princípio de que boa parte da informação em um pacote encapsulado com IP-em-IP é redundante. Portanto, ele apenas acrescenta uma nova informação de cabeçalho que é diferente da que foi incluída no cabeçalho IP original. Consequentemente, o encapsulamento mínimo apenas muda o endereço fonte e destino e coloca o endereço original em outro lugar do pacote. Isto requer apenas 8 a 12 *bytes* de sobrecarga no tunelamento. No entanto o encapsulamento mínimo é menos robusto, pois o Tempo De Vida (*Time To Live*) do pacote não é protegido, e o mesmo pode não sobreviver à fragmentações através da rede. Finalmente o encapsulamento de roteamento genérico foi projetado de forma que qualquer protocolo possa ser usado dentro do pacote encapsulado. Ele sofre de uma sobrecarga maior que o IP-em-IP, mas ao contrario dos outros ele suporta qualquer outro protocolo. Ele tem suporte para condições de encapsulamento recursivo, nas quais pacotes tunelados reentram continuamente no mesmo túnel antes de saírem.

2.5 Mudanças com o IPv6

O IPv6 inclui várias outras características para suporte à mobilidade, incluindo Autoconfiguração de Endereços Estáticos e Descobrimento de Vizinhança. O IPv6 também simplifica drasticamente o processo de renumeração, que pode ser crítico para a rotabilidade futura da Internet. Por causa do número crescente de computadores móveis acessando a Internet, um suporte eficiente à mobilidade fará uma diferença decisiva no desempenho da rede.

O suporte à mobilidade no IPv6 (IPv6 Móvel), como proposto pelo grupo de trabalho do IP Móvel (*Mobile IP working group*), segue o projeto do IPv4 Móvel. Mantêm-se as idéias de rede de origem, agente de origem, e o uso de encapsulamento. Como a descoberta do endereço de tratamento ainda é necessária, um nó móvel pode configurar seu endereço de tratamento usando a Autoconfiguração de

Endereço Estática e a Descoberta de Vizinhança. Portanto, os agentes externos não são mais necessários para o suporte à mobilidade no IPv6. O tunelamento com encapsulamento IPv6-em-IPv6 também é especificado.

2.5.1 Otimização de Rota

O suporte a mobilidade no IPv6 traz as idéias de otimização de rota sugeridas para o IPv4, como o envio de atualizações de ligação diretamente ao nó correspondente. Quando se sabe do atual endereço de tratamento do nó móvel, um nó correspondente pode enviar pacotes diretamente ao nó móvel sem a assistência do agente de origem. A otimização de rota aumenta o desempenho de nós móveis em redes IPv6. Isto é possível pois o espaço de endereço do IPv6 (128 *bits*) é muito maior que o do IPv4 (32 *bits*). Uma pequena parte deste espaçamento é reservada para todos os endereços IPv4 existentes, e outra é reservada para o endereço de enlace local (*Link-Local address*). Apesar deste endereço não ser roteável, garante unicidade em um certo enlace, fazendo com que nós presentes em um mesmo enlace possam se comunicar sem o uso de roteadores.

2.5.2 Segurança

Uma das grandes diferenças entre o IPv6 e o IPv4 é que espera-se fortes características de autenticação e criptografia em nós IPv6. Isto simplifica o suporte à mobilidade IPv6, pois não terão que ser especificados no protocolo IPv6 Móvel. Mesmo com essas características de segurança no IPv6, entretanto, o grupo de trabalho do IPv6 Móvel recomenda o uso de procedimentos de autenticação o menos freqüente possível. A razão para isto é que bons procedimentos de autenticação vêm com custos de desempenho e não devem ser utilizados desnecessariamente.

2.5.3 Roteamento de Fonte

Ao contrário do IPv4, nós correspondentes não redirecionam pacotes para o nó móvel. Ao invés disto eles utilizam cabeçalhos de roteamento existentes no IPv6, que implementam uma variação da opção de roteamento de fonte no IPv4. Algumas propostas de suporte à mobilidade em IPv4 sugerem um uso similar de roteamento de fonte, mas dois problemas principais ainda existem [10]:

- A opção de roteamento de fonte do IPv4 requer que o receptor do pacote roteado siga o caminho reverso até a fonte para assim determinar os nós intermediários. Isto significa que o nós mal intencionados que estejam no caminho podem interferir. Este problema tem que ser resolvido com protocolos de autenticação;

- Os roteadores existentes têm um péssimo desempenho no manuseio de opções de rotas de fonte. Conseqüentemente, os resultados com o uso de outros protocolos que utilizam rotas de fontes não foram satisfatórios.

  Entretanto, esses problemas no uso de rotas de fonte não se aplicam ao IPv6, pois o mesmo elimina a necessidade de se fazer uma rota reversa até a fonte e faz os roteadores ignorarem as opções que não são de sua atenção. Conseqüentemente, os nós correspondentes podem usar cabeçalhos de roteamento sem penalidade para os roteadores. Isto permite ao nó móvel facilmente verificar quando um nó correspondente não tem o seu endereço de tratamento correto. Então, os pacotes entregues por encapsulamento ao invés de rotas de fonte, devem ter sido enviados por nós correspondentes que necessitam receber atualizações de ligação do nó móvel. Isto é uma outra diferença entre a otimização de rota no IPv4 e no IPv6, pois agora o nó móvel envia atualizações de ligação aos nós correspondentes e não apenas aos agentes de origem.

  Outras características suportadas pelo IPv6 Móvel incluem:

- *Handoffs* suaves, o que no IPv4 Móvel é especificado para os agentes externos como parte da otimização de rota;
- Descobrimento de agente de origem automática.

Capítulo 3

Análise de Cenário

O objetivo do grupo de trabalho do IETF não foi criar um padrão e sim uma especificação, pois para se chegar a um padrão são necessários vários testes de implementação até se chegar a um ponto estável. Então, como a especificação do IP Móvel esta gratuitamente disponível na página web do IETF[1], várias implementações estão disponíveis na Internet.

A abordagem de pesquisa deste trabalho foi primeiramente definir um cenário de implantação, definindo alguns parâmetros e requisitos que o sistema de IP Móvel a ser escolhido suportasse, para depois pesquisar e analisar os sistemas existentes.

3.1 Metodologia de Escolha

A abordagem para a definição do cenário de implantação foi a seguinte:

- Definição de uma aplicação a ser usada na rede que utilizaria o IP Móvel;
- Definir requisitos necessários para dar suporte à aplicação escolhida;
- Definição de uma topologia de rede a ser utilizada;

[1] `http://www.ietf.org`

- Definir requisitos para dar suporte à topologia de rede.

3.1.1 Tipo de aplicação e requisitos necessários

De modo geral, o tipo de aplicação a ter prioridade em nosso cenário são as que utilizam o protocolo RTP (*Real Time Protocol*), mais especificamente aplicações de VoIP (Voz sobre IP). Este tipo aplicação utiliza um fluxo de dados constante e intenso devido à necessidade de manter a execução em tempo real.

O problema para o IP Móvel, com relação a protocolos de tempo real, surge quando o nó móvel está se movimentando entre redes distintas. Normalmente o endereço IP do nó seria trocado e a conexão perdida, porém com o uso do IP Móvel ele mudaria de rede transparentemente, ou seja, sem a mudança de IP. Porém, fisicamente o nó móvel mudou o ponto de conexão, e o IP Móvel tem que fazer a busca pelo endereço de tratamento e o registro deste endereço o mais rápido possível para que o tunelamento de pacotes de sua rede anterior para a nova rede seja efetuado quase sem perdas de pacotes.

Ou seja, é necessário que o implementação de IP Móvel adotada efetue *hand-offs* rápidos, de modo a manter o fluxo de dados em tempo real o mais consistente possível. Não é admissível pausas longas em fluxos de voz maiores que 125ms, pois o sinal pode ficar incompreensível em alguns momentos, como durante a transição de uma rede à outra.

3.1.2 Topologia de rede e requisitos

O sistema a ser escolhido irá funcionar em um ambiente de rede sem-fio com dispositivos variados como nós móveis. Esses nós móveis podem utilizar qualquer sistema operacional, tais como Linux, Windows, Symbian, dentre outros. Além disso, o ambiente de rede sem-fio é heterogêneo, ou seja, utiliza diferentes tecnologias tais como Bluetooth e Wi-Fi. Portanto, o sistema de IP Móvel deve se adaptar as tecnologias de rede sem-fio, o que não deve ser problema, já que este

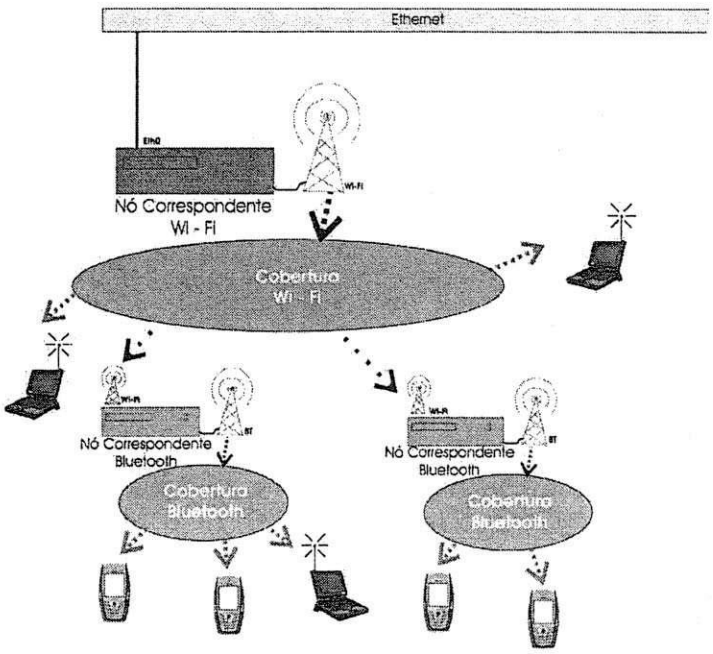

Figura 3.1: Topologia de rede proposta para análise de cenário

é o propósito das especificações feitas pela IETF. A arquitetura de rede pode ser ilustrada através da Figura 3.1.

O problema vem do suporte que o sistema de IP Móvel dá aos nós móveis. É necessário que o sistema de IP Móvel execute o software necessário para o funcionamento do nó móvel no maior número de sistemas operacionais possível, ou não dependa da execução de software algum nesses nós. Portanto para os nós móveis seria necessário que o sistema de IP Móvel funcione transparentemente, sem a necessidade de qualquer configuração extra.

3.2 Implementações pesquisadas e analisadas

Os sistemas de IP Móvel analisados funcionam no sistema operacional Linux, pois estes sistemas têm distribuição gratuita e de código aberto, característica comum as aplicações feitas para Linux. Isto facilita a análise do sistema e proporciona um melhor entendimento do sistema, pois seu código está à disposição para análise e

modificação, caso necessário.

Em uma pesquisa feita na Internet, os seguintes sistemas IP Móvel foram encontrados e considerados para uma análise mais específica:

- *The MosquitoNet Research Group* (Universidade de Stanford)[6];
- *The Monarch Research Project* (Universidade Carnegie Mellon) [5];
- *Dynamics - HUT Mobile IP* (Universidade de Tecnologia de Helsinki) [4];
- *Transparent Mobile IP - TMIP* (grupo de pesquisa SOWN) [1];

Outros sistemas foram encontrados, porém descartados da análise inicial por não terem uma boa documentação, estarem em estados iniciais de desenvolvimento, não funcionarem em Linux, dentre outros problemas.

A seguir, analisam-se rapidamente os sistemas escolhidos, observando se satisfazem os requisitos descritos na análise de cenário.

3.2.1 O MoquitoNet

A versão analisada foi a 2.0 beta. A implementação MosquitoNet Mobile IP é baseada nas especificações do IP Móvel do IETF. Todas as funcionalidades foram implementadas tanto no nó móvel quanto no agente de origem.

Esta implementação, entretanto, não provê uma implementação para o agente externo, dando toda ênfase à execução com endereço de tratamento arranjado (*collocated*), pois assim se elimina uma entidade no sistema. Ou seja, todo o processo de encapsulamento e desencapsulamento ocorre no nó móvel.

Esta é uma solução interessante, porém não preenche o requisito de topologia de rede, no qual vários dispositivos móveis com sistemas operacionais diferentes utilizariam à rede. O MosquitoNet apenas fornece versões em Linux e não tem um modo de execução sem a utilização de um *daemon* no nó móvel. Portanto este sistema foi descartado.

3.2.2 O Monarch

A versão utilizada foi a 2.0.0 alpha. O interessante desta implementação é a mistura de código em nível de usuário e em nível de *kernel*, o que aumenta o desempenho do sistema como um todo. Funções periódicas, tais como anúncios de agente, ou funções de controle, como gerenciamento de interfaces de rede e manuseio de registros, são executadas em nível de usuário como *daemons* em *background*, enquanto que funções como encapsulamento e desencapsulamento são implementadas no *kernel*. Outro atrativo deste sistema é o suporte a outros sistemas operacionais baseados em Unix, como o FreeBSD. Porém, esta implementação também utiliza endereço de tratamento arranjado (*collocated*), o que não satisfaz nossos requisitos.

3.2.3 O Dynamics

A versão analisada foi a 0.81. O principal aspecto dessa implementação é a utilização de uma versão hierárquica do IP Móvel, que distribui as funcionalidades dos agentes de mobilidade que estão perto do nó móvel. Este sistema satisfaz a necessidade de aumento de desempenho para *handoffs* rápidos e escabilidade. Toda a hierarquia é mantida sem o conhecimento do nó móvel. O protocolo proposto também provê segurança contra ataques de nós entre qualquer uma das entidades. Porém o maior atrativo desta implementação é o suporte a outros sistemas operacionais, em especial o Windows.

Apesar de se propor a funcionar tanto com suporte ao uso de endereço de tratamento arranjado, quanto com o uso de endereço de tratamento do agente externo, para total funcionalidade do sistema é sugerido o uso de endereço de tratamento arranjado e com isso enfrentamos no mesmo problema das implementações anteriores.

3.2.4 O Transparent Mobile IP

A versão analisada foi a 0.14 alpha. Apesar de ser uma implementação pouco desenvolvida, sua arquitetura tira toda a necessidade de configuração do nó móvel e à passa para outras duas entidades, que serão apresentadas no próximo capítulo. Esta característica resolve totalmente o problema existente com as implementações anteriores.

Apesar dessa implementação não seguir as especificações do IP Móvel sugeridas pela IETF, ela se encaixa em nossos requisitos, pois além de prover heterogeneidade de sistemas operacionais, este sistema foi feito para uma topologia de rede sem-fio.

Portanto a implementação de IP Móvel Transparente (TMIP) foi escolhida para implantação e estudo. Os detalhes da arquitetura, configuração e funcionamento, serão expostos no próximo capítulo.

Capítulo 4

O Transparent Mobile IP

O *Transparent Mobile IP* (TMIP) é um projeto de código aberto, que pretende resolver o problema de mobilidade entre redes separadas sem a necessidade de qualquer configuração no lado do cliente. O que separa este projeto do conceito de IP Móvel especificado pelo IETF é que este não requer nenhuma configuração ou alteração na pilha IP no lado do cliente. Isto implica que qualquer equipamento IPv4 funcionará normalmente. Ainda mais, o TMIP contém um servidor de DHCP integrado, que funciona como um servidor distribuído. Se um nó local está funcionando sem mais endereços livres para alocar a clientes que estão migrando para sua rede, ele pode simplesmente usar endereços de nós vizinhos.

Antes de começar a explicar o funcionamento e arquitetura do TMIP, vamos mostrar a terminologia deste projeto que difere um pouco da terminologia do IP Móvel. O TMIP basicamente consiste de três entidades:

Nó correspondente: é o principal conceito em uma rede TMIP. Um nó correspondente (CN) fica na margem das células móveis (i.e. os roteadores de borda) e serve todos os clientes móveis dentro das células. Eles devem identificar novos clientes e clientes migrados, e manipular a rede para assegurar que os clientes servidos mantenham a conectividade. Dentro de uma rede existem vários CNs.

Registrador de Localização Móvel: outro importante conceito é o do registrador de localização móvel (MLR). Existe apenas um MLR por rede móvel. Ele guarda detalhes sobre onde os clientes móveis estão ativos, e a alocação de endereços de cada cliente.

Estações Móveis: são correspondentes aos nós móveis do IPv4 Móvel. Uma estação móvel (MS) pode ser qualquer dispositivo que possa utilizar IPv4, e de fato não necessita ser móvel. Estações Móveis estão livres para sair da sua rede, e transparentemente migrar para outras redes. De fato, as estações se quer sabem que são móveis, pois estão sempre usando o mesmo endereço IP, e mandando tráfego para o mesmo *gateway* da mesma rede.

4.1 Funcionamento Básico do TMIP

Como foi dito anteriormente, a rede TMIP consiste de um MLR e de uma série de CNs. O MLR atua mapeando a atual localização e a alocação IP de cada cliente através de seu endereço MAC Ethernet. Cada CN tem anexado a si uma rede móvel, seja sem-fio ou não. Cada rede está em uma sub-rede diferente, e requer nível de roteamento 3 para se comunicar entre elas. Os nós móveis inicialmente aparecem em uma destas células, e obtém um endereço IP e uma alocação de rede. Sub-redes são usadas para cada nó móvel presente CN. Então cada nó tem uma máscara de rede, um endereço de rede dado, um endereço IP, um endereço *gateway* e um endereço de *broadcast* próprio.

Se este nó agora migrar para uma rede servida por um CN diferente, então esta migração será detectada pelo o novo CN, usando vários métodos tais como ARP, IP, DHCP, dentre outros. Este CN comunica-se com o CN de origem do nó móvel, e possivelmente o CN antigo de onde o nó móvel veio. Com uma simples transação de *handover* (distribuída em duas fases), o nó móvel estará presente em um novo CN, e a rede estará atualizada. Todo este processo acontece transparentemente

para o cliente.

Estas migrações não afetam as tabelas de roteamento da rede. Quando estiver remoto, os pacotes do nó móvel viajam normalmente. Entretanto, quando seu endereço fonte esta em uma CN diferente, pacotes de resposta não serão roteados diretamente. Com a ajuda do MLR, o CN de origem sabe a atual localização do nó móvel, e então encaminha, através de um túnel, os pacotes para o CN atual do nó móvel. Então o MLR atua como banco de dados para os CNs.

4.2 Vantagens do TMIP

Como dito anteriormente o principal objetivo para o TMIP é permitir aos clientes migrar entre redes sem a perca de conectividade. Isto tudo sem a necessidade de alterações no lado do cliente.

O TMIP também permite a alocação distribuída de endereços. Quando um cliente chega a uma célula móvel ele pode requisitar uma alocação de endereço de qualquer célula registrada na rede. Isto pode envolver um contato com o gerenciador do espaço de endereço, negociação de um túnel a ser usado, e finalmente atualizar a rede para permitir a passagem de tráfego. Outra maneira de alocação de endereço pode ser feita se o nó móvel registrar no MLR que sempre quer ser alocado com o mesmo endereço IP. Isto permite o registro desses nós em um DNS (*Domain Name Server*), por exemplo.

Com o TMIP também é possível rastrear nós. Ou seja, é possível saber onde cada nó está atualmente. Isto permite uma análise da rede para estabelecer características de carga e desempenho.

4.3 Topologia de rede utilizada

É possível utilizar o TMIP para várias topologias de rede diferente, por suas características flexíveis. Neste trabalho utilizamos uma topologia típica, que

consiste de um *backbone* Ethernet com pontos de acesso conectados a eles. Então, em algum lugar da rede, fixo, é colocado o MLR. Nos pontos de acesso Wi-Fi ou Bluetooth são colocados os CNs, como proposto na análise de cenário no capítulo anterior.

4.4 Configuração do TMIP

Parâmetros e requisitos necessários para instalação não serão discutidos pois fogem do escopo deste trabalho. Serão considerados apenas os aspectos de configuração levando-se em conta que o TMIP foi devidamente instalado.

Inicialmente apenas dois tipos de entidades são necessários para configurar o TMIP, que são o MLR e os CNs. Primeiramente irá se configurar o MLR e em seguida os CNs.

4.4.1 Configurando o MLR

Como foi dito, o MLR é o cérebro por trás do sistema. Basicamente o MLR guarda informações sobre os nós móveis através de seus endereços Ethernet MAC, seus endereços IP e localização atual. Estas informações podem ser de duas formas, dinâmicas ou estáticas. Uma informação dinâmica quer dizer que o nó está presente em algum lugar da rede naquele momento, enquanto informações estáticas podem ser usadas para que a rede tenha informações do nó quando este está *offline*.

O MLR também é o responsável por todas as alocações de endereço para clientes que estão migrando, implicando que toda a rede TMIP se transforma em um grande servidor DHCP distribuído.

Quando um nó móvel aparece dentro de uma célula, o MLR é utilizado para estabelecer sua identidade. Uma vez que as partes correspondentes tenham se comunicado e os túneis criados, o MLR é atualizado com a nova localização.

Em adição com a informação de localização, o MLR também lida com todas as alocações de endereço para os CNs.

É recomendado o uso de dois MLR. O MLR suporta um modo de *cópia de carbono*, que é semelhante à zonas de transferência dos DNS´s. Basicamente, um MLR primário irá transferir todos os dados dinâmicos e estáticos do nó móvel para um MLR secundário periodicamente. Isto significa que mesmo que o MLR primário seja desativado para uma nova instalação, quando ele funcionar novamente irá automaticamente puxar todas as informações do MLR secundário.

Primeiramente configura-se o MLR secundário. Na pasta de execução `tmip/mlrd` faz-se o seguinte. Cria-se um arquivo de configuração, o arquivo padrão é o `mlrd.rc` no qual deve-se fazer algumas alterações, mostradas a seguir:

```
network_name M-VoIP
port 5554
foreground false
log_file /var/log/mlrd.log
status_file /var/log/mlrd.status
log true
grant 150.165.61.143
```

A porta escolhida para o MLR secundário foi a 5554. A outra opção necessária é conceder (*grant*) direitos ao MLR primário especificando sua localização (IP ou nome DNS). Uma vez feita à configuração do MLR secundário, pode-se executá-lo em *foreground* ou não, utilizando o parâmetro -f, como mostrado a seguir:

```
[root@sip mlrd]$ ./mlrd -f mlrd.rc
```

Ao final da inicialização do MLR, a mensagem a seguir aparecerá indicando que o mesmo está em funcionamento:

```
+ MLR up and listening...
```

Agora o MLR está pronto e escutando sua rede para servir as requisições. Deve-se lembrar que todos os CNs devem usar o mesmo nome de rede.

Depois de configurar o MLR secundário, pode-se configurar o MLR primário, que deve estar em outro diretório. A configuração do MLR primário é ilustrada a seguir:

```
network_name M-VoIP
port 6554
foreground false
log_file /var/log/mlrd.log
status_file /var/log/mlrd.status
log true
cc_mlr 150.165.61.143:5554
```

Após configurar o arquivo de configuração, pode-se executar o MLR primário assim como executa-se o MLR secundário. Durante sua inicialização, o MLR primário indica se a cópia de carbono foi encontrada, como ilustrado a seguir:

```
+ Using carbon copy MLR server (150.165.61.143 on port 5554):  Seems
Ok.
```

Para verificar se o MLR primário e a cópia de carbono estão funcionando corretamente executa-se o comando `ccpush`, se a resposta for *Carbon copy push successful* então tudo ocorreu bem.

Aqui utilizamos os MLR secundário e primário no mesmo computador, mas nada impede de se executar os dois MLR em computadores separados.

O TMIP oferece vários comandos interativos (como `show, bindings`, etc.)

quando se executa o MLR no modo *foreground*. São na maioria comandos de depuração e são expostos na documentação do sistema TMIP.

4.4.2 Configurando os nós correspondentes

A aplicação do CN (`tmipd`) deve ser executada no *gateway* entre a interface de rede móvel e o resto da rede. Existem várias maneiras de configuração para uma rede. Neste trabalho consideramos que a interface móvel é sem fio (Wi-Fi ou Bluetooh), e a que vai para o resto da rede é uma interface Ethernet.

O arquivo de configuração é o `tmipd.rc` e deve ser alterado como o arquivo de configuração do MLR. Uma descrição detalhada das opções de configuração é descrita no cabeçalho do arquivo, mas a configuração básica é mostrada a seguir:

```
mlr 150.165.61.143
cn_name Primeira_CN
CN tunnel_prefix tmip0
cn_if eth0
mobile_if pan0
network_name M-VoIP
addr_pool pan0 * *
dns_server 150.165.61.3
log_file /var/log/tmipd.log
status_file /var/log/tmipd.status
debug_level 2
```

- Após o `mlr` coloca-se o endereço do MLR;
- após o `cn_if` coloca-se o nome da interface do CN (aqui a Ethernet - `eth0`);
- após o `mobile_if` coloca-se o nome da interface móvel (aqui um ponto de acesso bluetooth - `pan0`);

- e após o `network_name` coloca-se o nome da rede (aqui `M-VoIP`).

No campo `addr_pool` define-se o espaço de endereços a serem alocados na interface móvel. Pode-se alocar todo o espaço de endereços, nenhum endereço ou alguma faixa especifica. No campo `cn_name` define-se o nome do CN, e finalmente define-se o servidor DNS primário que será passado aos clientes via DHCP.

O campo `tunnel_prefix` serve para quando se for utilizar mais de um CN por nó físico, poder-se separar os túneis específicos para cada CN. Se apenas um CN é utilizado por máquina, basta usar o nome padrão.

Após configurar o arquivo `tmipd.rc`, pode-se executar o CN e verificar se ele visualiza o MLR e os outros CNs para assim criar túneis, ou seja, ver se o CN realmente funciona. Para isso, no diretório do tmipd execute a CN da seguinte maneira:

```
[root@sip tmipd]$ ./tmipd -Ef tmipd.rc
+ Starting TMip Correspondent Node [v0.14a]
+ Loading settings from configuration file...
 + Using mlrd.rc
Network Connectivity Evaluation
==============================
 + MLR @ 150.165.61.143:  Passed.
 + CN @ 150.165.61.143 [Second_CN]: Passed.
```

O comando -Ef serve para checar a conectividade do CN com os outros CN e o MLR. Agora se pode executar a aplicação do CN do seguinte modo:

```
[root@sip tmipd]$./tmipd -f tmipd.rc
```

Na inicialização do CN, o mesmo executa basicamente os seguintes passos:

- Executa um *controlador de túneis* que indica os tipos de túneis suportados pelo CN;
- Checa a conectividade com o MLR;
- Disponibiliza um espaço de endereço configurado no *script*;
- Inicializa o servidor DHCP, caso tenha sido configurado.

4.4.3 Funcionamento e roaming

Com os CNs e o MLR configurados e sendo executados, basta ligar o cliente DHCP no nó móvel e utilizar o TMIP. Pode-se colocar os endereços IP do nó móvel manualmente, porém deve-se seguir uma regra do TMIP. Como foi dito, no TMIP cada nó móvel tem uma sub-rede para si próprio, então deve-se configurar seus parâmetros do modo que o TMIP espera: escolhe-se um endereço qualquer e faz deste o endereço de rede do nó (N), em seguida se define o endereço IP como N+1, o gateway como N+2 e o endereço de broadcast como N+3.

Quando um nó móvel se conecta ao um CN, ele recebe uma alocação de endereços como descrita anteriormente. Enquanto isso o CN registra este nó móvel com a MLR. Ao final da operação o CN indica que o nó móvel está em sua sub-rede, como descrito a seguir:

```
-> Mobile host [00:02:c7:19:b3:d0] has arrived in this cell
```

Após ter-se registrado em um CN o nó móvel pode migrar para outro transparentemente. Nesta mudança, o novo CN ao qual o nó móvel está migrando pergunta ao MLR qual o CN anterior do nó. Ao receber esta informação, ele contata o CN anterior, o informa sobre o processo de *handover*, cria um túnel entre eles, e recebe os parâmetros de configuração do nó móvel. Por final, o CN informa o MLR sobre as mudanças ocorridas.

Portanto o nó móvel migrou de um CN para outro transparentemente, mantendo todas as suas configurações de sub-rede.

Agora, todos os sistemas estão configurados e funcionando corretamente. Existem outros modos de execução que o TMIP suporta, dentre eles se destaca o modo registrado no qual apenas as estações móveis com endereços Ethernet MAC previamente registrados podem acessar a rede. Este é um modo interessante de uso, porém foge do escopo deste trabalho.

Capítulo 5

Conclusões e Futuros Trabalhos

A partir do estudo das especificações do IETF para o suporte à mobilidade com o IPv4 Móvel, observamos que ao mesmo tempo em que estas especificações nos dão uma ferramenta muito poderosa para novos tipos de aplicação, também nos dão muito espaço para o acréscimo e aperfeiçoamento das técnicas de autenticação e registro.

Isto foi comprovado com a análise das implementações do IPv4 Móvel disponíveis na Internet. Cada uma dessas implementações tem características próprias, que aparecem como soluções para problemas que não foram solucionados na especificação, ou simplesmente como sugestões para a otimização do desempenho do sistema como um todo.

Com esta pesquisa fomos capazes de, a partir de parâmetros de comparação e escolha definidos previamente, escolher um sistema flexível o suficiente para se adaptar à realidade de nossa pesquisa. Com o intuito de que fosse possível fazer um estudo e análise mais detalhada de um sistema.

Uma dos pontos interessantes de nossa pesquisa foi a escolha de um sistema de IP Móvel que não implementa as especificações do IETF. Essa implementação utiliza os mesmo conceitos de funcionalidade do IPv4 Móvel especificado pelo IETF como o conceito de túnel IP-IP e encapsulamento IP-em-IP, porém com

entidades diferentes (apenas duas entidades ao contrário das três entidades do MIP).

A configuração do *Transparent Mobile IP* e suas funcionalidades foram estudadas e analisadas detalhadamente, observando-se todos os passos realizados pelo sistema e sua abordagem de sub-redes individuais para o provimento de mobilidade à estações móveis. Este sistema utiliza uma arquitetura bastante semelhante a dos sistemas de telefonia celular existentes, tais como a entidade MLR, que tem funcionalidades bastante semelhantes à entidade HLR de sistemas celulares, e o conceito de cobertura a partir de células.

5.1 Futuros Trabalhos

Os próximos passos serão a implantação efetiva do sistema, que seria embarcá-lo em um dispositivo com sistema operacional Linux e integrá-lo com *gateways* específicos dentro do projeto M-VoIP. Depois, serão realizados testes com dispositivos móveis, tais como PDA´s e celulares com interfaces Bluetooth e Wi-Fi, utilizando-se aplicações que utilizam protocolos de tempo real, como aplicações de VoIP.

Deste modo, chegamos a um conhecimento mais abrangente dos sistemas de IP Móvel existentes, para que se a utilização do TMIP não seja satisfatória, podermos simplesmente implantar outro sistema disponível, ou até mesmo implementar uma versão própria que se adapte a nossas necessidades.

Bibliografia

[1] Transparent Mobile IP. `http://www.slyware.com/projects_tmip.shtml`.

[2] Andrew F. Myles Charles E. Perkins. Mobile IP. 1996.

[3] S.E. Deering. ICMP Router Discovery Messages, IETF RFC 1256, Setembro 1991. `http://www.ietf.org`.

[4] Dan Forsberg, Jari T. Malinen, and Jouni K. Malinen. *Dynamics - HUT Mobile IP technical document.* Helsinky University of Technology, Outubro 1999.

[5] David A. Maltz and David B. Johnson. *The CMU Monarch Project IETF Mobile IPv4 Implementation User´s Guide*, Janeiro 1998.

[6] Mobile Computing Group of Stanford University. *MosquitoNet Mobile IPv4 - User´s Manual*, 2.0 beta edition.

[7] Charles E. Perkins. IP encapsulation within IP, IETF RFC 2003, Outubro 1996. `http://www.ietf.org`.

[8] Charles E. Perkins. IP mobility support, IETF RFC 2002. Outubro 1996. `http://www.ietf.org`.

[9] Charles E. Perkins. Minimal encapsulation within IP, IETF RFC 2004, Outubro 1996. `http://www.ietf.org`.

[10] Charles E. Perkins. Mobile networking through mobile IP. *IEEE Internet Computing*, 1998.

[11] J. Redi and P. Bahl. Mobile IP: A solution for transparent, seamless mobile computer communications. *Fuji-Keizai's Report on Upcoming Trends in Mobile Computing and Communications*, 1998.

[12] R.L. Rivest. The MD5 Message-Digest Algorithm, IETF RFC 1321, Abril 1992. `http://www.ietf.org`.